Coverless Data Hiding in VoIP based on DNA Steganography with Authentication

Deepikaa Soundararajan
School of Computer Science and Engineering
Vellore Institute of Technology, India
deepikaa.s@vit.ac.in

Saravanan Ramakrishnan
School of Computer Science and Engineering
Vellore Institute of Technology, India
rsaravanan@vit.ac.in

Abstract: *Data hiding in Voice over Internet Protocol (VoIP) using coverless approach improves the undetectability by preserving the cover bits from modification. This paper focuses on hiding the secret message in VoIP streams using Deoxyribonucleic Acid (DNA) steganography approach. DNA steganography is known for its low cracking probability. The embedding process is done in two steps. The first step converts the VoIP sample, secret message and a user generated key (for Authentication) into m-RNA pattern during transcription and the second step converts the m-RNA to form a triplet during translation process to create a protein array, where the secret message is embedded. The secret message is extracted from the protein array by applying reverse translation and Transcription. The proposed approach improves the undetectability by leaving the cover bits unmodified with Perceptual Evaluation of Signal Quality (PESQ) values 84% comparatively greater than the state of art techniques.*

Keywords: *DNA, VoIP, coverless approach, data hiding, steganography.*

Received March 27, 2021; accepted March 17, 2022
https://doi.org/10.34028/iajit/20/2/5

1. Introduction

Steganography conceals the secret message into a cover object. Digital steganography hides the secret bits in digital cover file. The digital cover may be static or dynamic. The static covers such as image, audio and video have the fixed statistical properties. Steganography on image [2, 4, 16], audio [11, 14], video [15] methods achieve good bandwidth. However, the digital files undergo changes that in turn affects the statistical properties of the file. The statistical analysis on such covers may exploit the algorithm and the secret bits. There are few works, which mainly aimed to reduce the embedding rate, such as Exploiting Modifications Directions (EMD), which was initially implemented in images to reduce the number of alterations made to the cover file, was later implemented in audio files to reduce the alterations done [7].

The dynamic covers like as network headers, audio and video data packets [5, 17, 21] have varying statistical properties because of its dynamic nature. The hacker with no sufficient knowledge about the dynamic cover, as well as the algorithm are unable to plan attack on cover areas thus reducing the chance of algorithm and cover exploitation and the extraction of secret message. The dynamic nature of internet packets attracts the researchers to use it for covert communications.

Voice over Internet Protocol strives (VoIP) to be one of the cheapest means of communication in the digital era. VoIP steganography conceals the secret messages in the streaming VoIP conversation. VoIP uses the packet switching technology, where the voice packets are transferred from sender to receiver via internet. VoIP Steganography uses these VoIP packets as cover to hide messages.

VoIP steganography survey [8, 22] discussed three ways in hiding the messages in VoIP. The VoIP data hiding method includes hiding the data in the payload, hiding the data in the unused header fields by changing the timing relations and sometimes the combinations of both. The payload embedding methods mainly use Least Significant Bit (LSB) modification with various flavors like Partial Similarity Value (PSV) [31], The voice quality degradation is reduced by avoiding the number of modifications made using the matrix embedding process [34], The combination of Partial Similarity Value (PSV) and matrix embedding yielded a good embedding capacity [32] and Quantization Index Modulation [33] provides more bandwidth to hide the data bits. However, modifications done to the payload deteriorates the audio quality. [20] Another approach of using timing relations to hide the secret messages into the delayed packets proved to resist steganalysis.

The next dimension of steganography is coverless steganography, where a new approach is applied to hide the secret messages with no modifications done to the cover during embedding. This approach preserves the statistical properties from leaking the existence of secret bits thereby improving undetectability and transparency. This approach has been implemented in

images. Studies on the coverless approach show two basic methods of embedding. The first method hides the secret messages using the hashing technique [38, 39, 40, 41, 42]; the pixel matching the secret message is selected based on the hash functions. The later method focuses on hiding secret bit using texture synthesis technique [36, 37], where the texture of image is synthesized based on the matching features of secret message.

The first coverless approach in VoIP was implemented using hashing technique [10]. A hashing function is applied to VoIP samples that aids in cover bit selection. The selected cover bits hide the secret messages on a condition. The hashing also helps to identify the hidden bits during extraction.

Table 1. Translation table (combination of 3 nucleotide gives an amino acid).

1st B \ 2nd B	U		C		A		G		3rd B
U	UUU UUC	PHE	UCU UCC UCA UCG	SER	UAU UAC	TYR	UGU UGC	CYS	U C A G
	UUA UUG	LEU			UAA UAG	STOP	UGA UGG	STOP TRP	
C	CUU CUC CUA CUG	LEU	CCU CCC CCA CCG	PRO	CAU CAC	HIS	CGU CGC CGA CGG	ARG	U C A G
					CAA CAG	GIN			
A	AUU AUC AUA	LLE	ACU ACC ACA ACG	THR	AAU AAC	ASN	AGU AGC	SER	U C A G
	AUG	MET			AAA AAG	LYS	AGA AGG	ARG	
G	GUU GUC GUA GUG	VAL	GCU GCC GCA GCG	ALA	GAU GAC	ASP	GGU GGC GGA GGG	GLY	U C A G
					GAA GAG	GLU			

The paper is organized as follows, section 2 describes the fundamentals of DNA translation and transcription. Section 3 highlights some important research works carried in DNA steganography. Section 4 showcases the observations and the performance of the method. Section 5 summarizes the research work carried in this paper.

2. Overview of DNA Translation and Transcription

The proposed coverless approach using Deoxyribonucleic Acid (DNA) steganography process requires the understanding of DNA translation and DNA Transcription to perform the embedding and extraction. This section provides the basic knowledge upon protein synthesis. In biological term, DNA carries the genetic information from parent to offspring. Each DNA is represented as 4 nitrogen bases namely Adenine (A), Guanine (G), Cytosine (C) and Thymine (T) [6]. The Ribonucleic Acid (RNA) is responsible for the synthesis of various proteins according to the genes. This conversion of DNA to its corresponding protein based on the genetic code is taking place in two steps called translation and transcription.

Transcription-In this process, DNA is transferred to mRNA by Complementary base pairing method. Translation-In this process, mRNA synthesizes corresponding protein. Three bases (triplet code) are assembled together to form an amino acid. The chain of amino acids forms a protein.

Each triplet combination synthesizes an amino acid. Table 1 describes the combination of nucleotides and the amino acid synthesized from it. The triplet can form a range of twenty amino acids. Same amino acid can be generated from different combinations of codons. Basically, there are 4 nitrogen bases, from which 64 base codons (triplets) can be obtained. From these 64 codons, 61 codons only generate amino acids. The amino acids synthesized in a sequence to form a protein. Normally a protein starts with AUG, which is an initiation codon. UAA, UAG, and UGA are termination (stop) codons. After the termination codon, the sequence breaks and a new sequence is initiated for a new protein.

3. Related Works

DNA steganography aims at hiding the secret messages in DNA sequences. The DNA sequences may be original or fake DNA sequences created as a result of embedding algorithm. DNA steganography proved to have a low cracking probability. Hamed *et al.* [13] reviewed few works on DNA steganography based on the computations of cracking probability. The original and faked DNA sequences have no difference and also the DNA sequences can be of any length. The DNA steganography provides large storage capacity. Hence used in various data hiding methods. Al-Harbi *et al.* [3] have analyzed the pros and cons of the existing data hiding methods using DNA steganography. Based on the survey Shiu *et al*. [29] have DNA steganography can be broadly classified into three methods based on the embedding process as shown in Figure 1.

3.1. DNA Substitution Methods

The simplest method of hiding the secret message based on a substitution table framed by the author. Based on the DNA substitution table, the secret message is substituted by the matching DNA sequence. Each algorithm frames different substitution table. Some approaches substitute the secret message by the

DNA triplets as per the substitution table. As a result, the new DNA sequence is created. This DNA sequence will be sent directly or concatenated with the cover reference DNA sequence.

Agrawal *et al*. [2] proposed a dictionary-based substitution table that mapped the triplet codons to six bit binary information. The secret message is converted to binary bits, which is substituted by triplet codon to produce a fake DNA sequence. The DNA sequence is then hidden into a string at different intervals generated by quadratic residue generator.

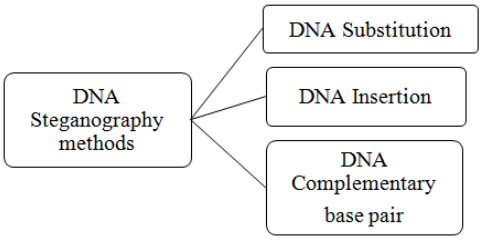

Figure 1. Types of steganography methods.

Marwan *et al*. [19] proposed an improved DNA based steganography, where the DNA - Play fair cipher proposed by Abbasy *et al*. [1] was improved with simple pre-processing steps. The ciphered DNA sequence is hidden using the substitution technique. As a result of this improved DNA-Playfair cipher, the data hiding capacity is improved 25% than the original method. Farhan *et al.* [12] have collaborated the idea of S-Boxes, into the DNA Steganography to obtain a faster and optimal solution. These S-Boxes play an important role in block cipher techniques in cryptography.

Wang *et al.* [35] used the substitution technique to frame DNA sequence using a dictionary and then inserted into the cover using a microdot technique. Based on a prediction, security is analyzed and further decomposed to attain the desired security. Sushma *et al*. [30] similar case of DNA encryption is designed, such that the message is converted into a binary sequence and then into DNA sequences, which is then embedded into a image to achieve additional security.

3.2. DNA Insertion Method

Initially the secret message is converted into the binary format and then the binary sequence is converted into the DNA format. These DNA sequences are inserted into the cover reference DNA sequences and sent to the receiver.

Malathi *et al*. [18] improved the DNA insertion algorithm from the dictionary-based substitution method. The bases were directly substituted by the data as per the dictionary. The improved insertion algorithm used two keys to improve the security of the algorithm. The first key is XORed with the first binary sequence of the secret message. The resulting sequence is iteratively XORed with the next binary sequences. The cover DNA is converted into binary sequence and splitted into sequence based on second key. Each bit of the encrypted cipher is inserted into the cover DNA binary sequence based on the dictionary-based substitution method.

Na [25] inserted the encrypted nucleotide into the SNP regions of genome, which is naturally polymorphic and hence difficult to identify the presence of message. The added feature is the checksum attached to detect the noise induced errors.

3.3. DNA Complementary Base Pair Method

The secret message is first converted into the binary sequence, and then into DNA sequences from the digraphs. The complementary base pair for the DNA sequence is generated. This method supports coverless approach, where the matching cover DNA sequence is identified and the reference is sent to the receiver. Mitras and Aboo [23] uses the DNA sequences to identify the matching complementary sequence to hide the secret message from DNA database.

Mohammed *et al*. [24] used neural networks to achieve a highly secured cipher text. First phase converts the secret message into DNA sequence. Second phase selects the reference DNA phase. The third phase hides the nucleotide base of the message into matching nucleotide base of reference DNA phase from backside. The index of the matching reference phase is noted in an array and the index is converted to binary sequence. Neural network back propagation algorithm is trained to embed the secret message DNA into the reference DNA. The calculated weights are sent to the receiver, from which the secret message is extracted.

Nisperos *et al*. [26] proposed the DNA steganography with a coverless approach, so as to strengthen the algorithm by nil modifications to the cover image. Initially the secret image to be transferred is converted to DNA pattern and a key value is generated with a timestamp value. Both the secret image DNA pattern and the Key value DNA pattern are XORed to increase the confidentiality. The stego-image is generated by complementing the resultant DNA pattern and the transcription and the translation is applied on the subsequent results. The X and Y coordinates are identified from the pairs of proteins and codons. Then the reverse process of translation, transcription and complementing will result in the encrypted DNA pattern which can be decrypted with the key.

The DNA Steganography methods discussed above are applied to image, audio. They don't suffer any timing restrictions for embedding and extraction and computational complexity increases the security. The security plays a motivational factor in choosing DNA steganography for VoIP. However, the proposed approach on VoIP has a timing restriction as the real

time streaming packets should not allow delay in packets due to embedding.

4. Proposed Algorithm

The proposed algorithm embeds the secret message in VoIP using DNA transcription and translation. The resulting protein is shared with receiver from which the secret message is being extracted. Embedding process takes three inputs such as VoIP sample, secret message and a key known only to the sender.

4.1. Voip Frame Selection

VoIP audio streams are organized in the form of VoIP packets. Each packet has a VoIP frame with n samples (say n=1024) with m bits/sample (say m=8). The major challenge with VoIP is it's dynamic nature and time synchronization. It demands less computation time and also negligible time delay during the embedding process and also successful extraction of secret message at the receiver side.

The proposed algorithm in Figure 3 aims to reduce the computational time and also embedding process should not cause an unwanted time delay during embedding. In order to achieve this goal, the embedding process hides secret message only on selected sample in a frame. There can be two approaches such as fixed frame selection such as selecting particular i^{th} sample in every frame. Another approach may use certain criteria or function to select a sample from each frame [9, 31, 32, 33]. Comparing the two approaches the later one seems to be less susceptible.

4.2. Embedding Algorithm

The proposed coverless approach of DNA steganography in VoIP aims at improving the undetectability and security by combining the DNA substitution and DNA complementary base pair method. All the previous works embedded the secret message into DNA sequence of a cover image or audio completely. A base from DNA sequence of VoIP sample, secret message and the secret key are used in a combination to form a triplet. Hence the partial knowledge of any one of these will not reveal the secret information. The Figure 2 shows the embedding steps and are explained as follows.

- *Step* 1: Convert the secret message into binary sequence. S= {s_1, s_2….. s_n}, where n is the length of secret message.
- *Step* 2: Perform the XOR with the secret message and secret key for additional security.
- *Step* 3: Convert the resulting binary sequence of secret message into DNA sequence based on the Table 1. Every 2 bits of binary sequence such as (s_1s_2) = (00) is mapped to a DNA base codon 'A' as shown in Table 2.

Table 2. DNA-Binary mapping table.

DNA Base	Binary code
A	00
T	01
G	10
C	11

- *Step* 4: Perform transcription on the DNA sequence to convert it to mRNA.
- *Step* 5: Convert the secret key into binary sequence K= {k_1, k_2,…., k_m}, where m is the length of secret key. Repeat the sequence to match the length of the secret message.
- *Step* 6: Complement of this binary sequence of secret key. Convert the resulting binary sequence of secret key into DNA sequence based on the Table 1. Every 2 bits of binary sequence is mapped to a DNA base codon
- *Step* 7: Perform transcription on the DNA sequence to convert it to mRNA.
- *Step* 8: Initiate the VoIP call. The VoIP packets are splitted into VoIP frames and each Frame has p samples.
- *Step* 9: Select the sample based on the criteria. The VoIP sample is converted into binary sequence and V= {v1, v2,.., vn}.

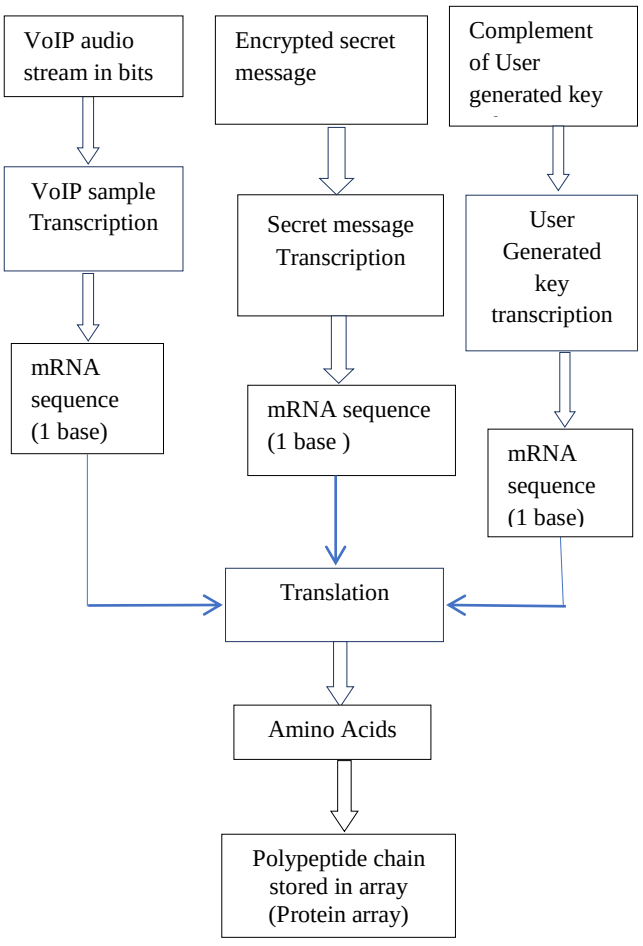

Figure 2. DNA embedding algorithm.

- *Step* 10: Perform transcription on the VoIP DNA sequence to convert it into mRNA.
- *Step* 11: Extract 1st base of mRNA of secret message, VoIP sample and secret key to form a triplet.
- *Step* 12: Based on the translation table given. The corresponding amino acid is stored in the array.
- *Step* 13: The protein array is sent to the receiver.

The proposed method does not completely rely on the VoIP sample but also uses a secret key thereby increasing the security. Partial knowledge of VoIP samples does not exploit the final protein synthesized, as the same protein can be synthesized from different combinations of triplets.

4.3. Extraction Algorithm

The proposed algorithm in Figure 4 is designed based on the blind approach. The advantage of this novel approach is that the secret message extraction doesn't depend on the VoIP cover. The protein array is sufficient enough to extract the secret message, if the recipient has the knowledge of algorithm. The transfer of protein array is not under the scope. To ensure the safety and security of the key, the protein array can be encrypted using any of the effective encryption algorithms. The secret key needed for the extraction is hidden in the protein array. It is assumed that the sender and receiver have the knowledge of working mechanism of the algorithm.

- *Step* 1: The receiver now has the secret key and protein array.
- *Step* 2: The protein array undergoes the reverse translation. Extract the second bit from the triplet subset.

For each amino acid in the protein array to be synthesized, a subset of triplet codons combinations are identified from the translation table. In the embedding algorithm the triplets were derived from three different covers. (1st base from VoIP sample, 2nd base from secret message, 3rd base from the secret key).

On careful observation of the triplet combination, the second triplet remains the same for each amino acid except for a particular type of protein. From the embedding algorithm, we understood that the secret message is hidden in the 2nd base of the triplet.

- *Step* 3: The extracted base nucleotide is stored in the array. The base nucleotide is in the mRNA format.
- *Step* 4: The base nucleotides undergo a reverse transcription to convert mRNA to DNA.
- *Step* 5: The DNA is converted to the binary sequence based on the substitution table.
- *Step* 6: The steps through 2 to 5 are repeated for the third bit. The reverse transcription is done to convert the DNA to binary sequence.
- *Step* 7: Perform complement to the resulting binary sequence to obtain the secret key for authentication and decryption.
- *Step* 8: The binary sequence of step 5 is XORed with the secret key to decrypt the secret message.

Thus the secret message extraction is successfully done without disturbing the cover bits.

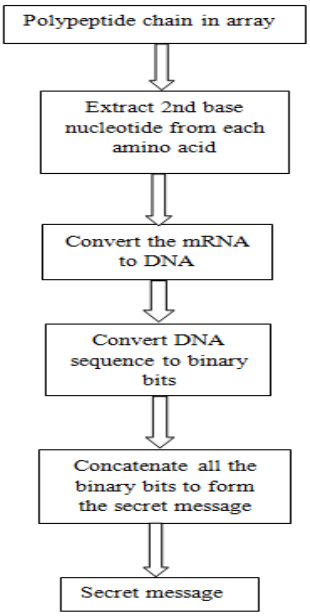

Figure 3. DNA extraction algorithm.

5. Experimental Results

DNA steganography based on coverless approach proposed in this paper is implemented using a VoIP prototype is developed based on UDP protocol in MATLAB within a local network. The DNA Steganographic embedding and extracting algorithms were implemented as functions and called from VoIP prototype. Before the VoIP Call is initiated, the Transcription function is applied to the secret message and secret key, which in turn is converted to form m-RNA sequence to reduce the computation complexity during the embedding process and to avoid the delay.

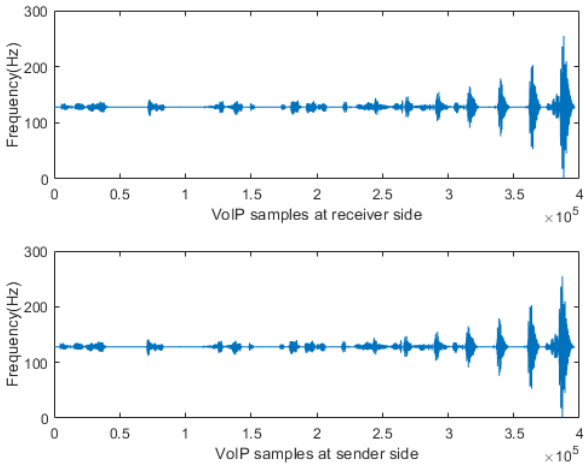

Figure 4. VoIP samples at both sides.

After the VoIP call is initiated, the selected VoIP sample undergoes transcription and translation resulting in amino acid formation. Figure 5 shows the plot of VoIP samples at both sender side and receiver side after embedding and before extraction of 10s real-time voice recorded and embeds 15B of secret message in it. The other advantage of this approach is that, while extracting the secret message, the third base codon of the triplet gives an authentication of the trusted sender and proves that the message is not intercepted by an intruder.

The performance of the proposed approach is compared between the covered and coverless methods based on Perceptual Evaluation of Signal Quality (PESQ) in Figure 6 and capacity in Table 3. The covered methods include the traditional LSB and the matrix embedding [27]. The coverless methods include the hashing technique [9] and the proposed approach.

5.1. Histogram

Histogram is one of the metrics to detect the presence of bits during steganalysis. The changes made to the samples during embedding, may differ in the frequency range that will reflect in histogram plot. The histogram plotted in the Figure 5 proves that the VoIP samples at the sender side and the samples at the receiver side have not been modified and quality of VoIP call is not degraded.

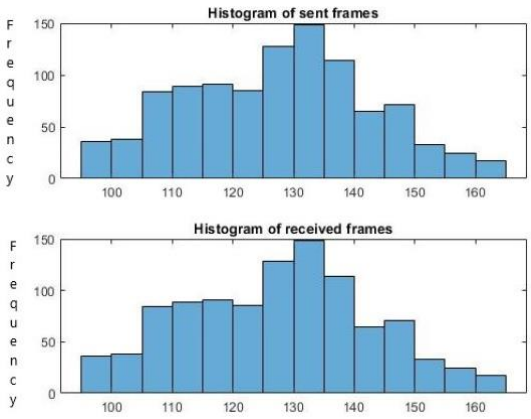

Figure 5. Histogram at both communicating ends.

5.2. PSNR

Peak Signal to Noise Ratio represents the difference in the original speech signal and noised speech signal. PSNR is calculated using the Equation (1).

$$PSNR = 20.log10\left(\frac{Max}{\sqrt{MSE}}\right) \quad (1)$$

This can also be represented as

$$PSNR = 20.log10(Max) - 10.log10(MSE) \quad (2)$$

Where Mean Square Error (MSE) between original and noised signal and max is the total number of bits used to represent a signal and is calculated by the Equation (3).

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[s(i,j) - r(i,j)]^2 \quad (3)$$

Salomon [28] When the original and noised signal does not differ, the Mean Square Error (MSE) is zero and hence PSNR will result in infinity on computing Equation (1). So the Equation (2) is considered where 10.log 10(MSE) becomes 0 and the PSNR yielded is 48db.

5.3. PESQ

PESQ is an objective method to measure speech quality using Mean Opinion Score (MOS) and Listening Quality Objective (LQO). PESQ is represented in a scale from 1 to 5. The higher the score, the higher the quality of the speech signal. The Proposed algorithm yielded a PESQ score of around 4-4.3 for the recorded speech files at the sender side and receiver side.

The PESQ results are analyzed with the real time audio recordings. Table 4 shows the comparison of the covered methods such as the traditional LSB and Matrix embedding approach and the coverless methods such as the hashing and the proposed approach. Figure 6 shows the coverless methods achieve a higher PESQ values than the covered methods and the proposed approach proved to have a good audio quality.

Table 3. Comparative results of PESQ between covered and coverless methods.

	LSB	ME [27]	Hashing [9]	Proposed method
PESQ MOS	3.437	4.121	4.254	4.279
MOS LQO	3.508	4.003	4.379	4.463

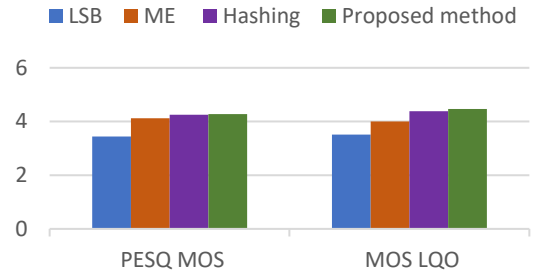

Figure 6. Comparison of PESQ between covered and coverless methods.

5.4. Capacity

The capacity represents the number of bits hidden per VoIP sample. The VoIP sample consists of 8 bits, which forms a sequence of 4 nucleotides. The MSB is considered here for embedding, i.e., the first nucleotide (left to right) is used for embedding. Normally, LSB is preferred in state of art techniques. To avoid hacker's attention towards LSB, the MSB is considered. A triplet is formed by combining 6 bit from the cover (2 VoIP MSBbits+2 msg bits+2 key bits). The translation synthesizes an amino acid.

Each amino acid carries a nucleotide of the secret message. Each nucleotide is represented by a digraph

(2 bits of the binary sequence). Hence the capacity can be derived as 2 bits per sample. For each VoIP frame, 1-2 samples are selected. For a 10S conversation, the VoIP frames transferred ranges around 400-450. The number of secret bits hidden in10s of Conversation ranges from 1K to 1.8Kb. The comparison of capacity between the covered and coverless methods are analyzed with respect to bit change rate and embedding rate as in Figure 7.

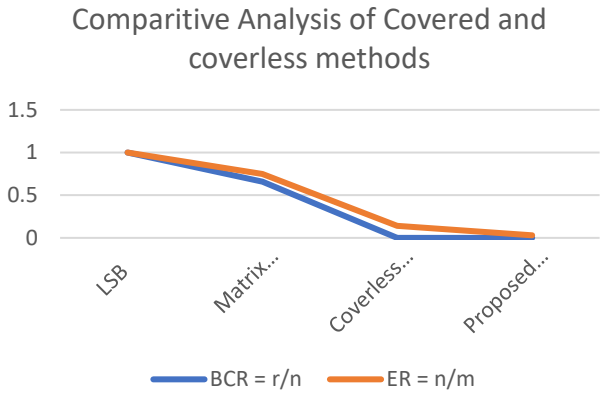

Figure 7. Comparison of BCR and ER between covered and coverless methods.

Table 4. Analysis of capacity of covered and coverless methods.

Data Hiding Methods	Secret message length (n)	Cover bit modified (r)	Cover bits (m)	BCR = r/n	ER = n/m
LSB	120	120	120	1	1
Matrix Embedding using Random binary matrix [27]	120	~80	160	0.66	0.75
Coverless Hashing approach [9]	120	0	840	0	0.14
Proposed DNA Steganography method	120	0	3072	0	0.03

On analyzing the bit change rate the coverless methods do not modify the bits and hence the value remains zero. The embedding rate is the main factor that measures the capacity achieved. LSB and Matrix Embedding (ME) methods yield a 80 to 90 percent higher capacity than the coverless methods. The capacity of the proposed approach is much smaller than the covered approaches. This is because the coverless approaches hides the bits in selected samples such that the covers are not disturbed.

6. Conclusions

The data hiding in VoIP conversation using coverless approach based on DNA steganography is proposed and implemented. The performance is analyzed in terms of statistical property preservation using histogram (undetectability), Bit Change Rate (BCR) and Embedding Rate (ER) (capacity) and (PESQ) audio quality. The statistical properties of the cover are preserved and the secret key is used to enhance the security of the secret message. Thus, the statistical steganalysis cannot reveal the presence of secret message based on the statistical properties. This approach hence achieves undetectability. One of important fact to be considered is the transfer of protein array. The protein array cannot be attached to cover, which may attract hacker's attention. Hence the protein array needs to be shared individually, apart from VoIP conversation. The results of comparison between the covered and coverless methods show that the proposed coverless methods may have less embedding rate than the covered methods, but the PESQ values show that the quality of the audio is not compromised. The future works may contribute in increasing the capacity without comprising the quality and also preserve the statistical properties of the cover.

References

[1] Abbasy M., Nikfard P., Ordi A., and Torkaman M., "DNA Base Data Hiding Algorithm," *International Journal on New Computer Architectures and Their Applications*, vol. 2, no. 1, pp. 183-192, 2012.

[2] Agrawal R., Srivastava M., and Sharma A., "Data Hiding Using Dictionary Based Substitution Method in DNA Sequences," *in Proceedings of 9th International Conference on Industrial and Information Systems*, Gwalior, pp. 1-6, 2014.

[3] Al-Harbi O., Alahmadi W., and Aljahdali A., "Security Analysis of DNA Based Steganography Techniques," *SN Applied Sciences*, vol. 2, no. 2, pp. 1-10, 2020.

[4] Anees A., Siddiqui A., Ahmed J., and Hussain I., "A Technique for Digital Steganography Using Chaotic Maps," *Nonlinear Dynamics*, vol. 75, no. 4, pp. 807-816, 2014.

[5] Bąk P., Bieniasz J., Krzemiński M., and Szczypiorski K., "Application of Perfectly Undetectable Network Steganography Method for Malware Hidden Communication," *in Proceedings of 4th International Conference on Frontiers of Signal Processing*, Poitiers, pp. 34-38, 2018.

[6] Balado F., "Capacity of DNA Data Embedding Under Substitution Mutations," *IEEE Transactions on Information Theory*, vol. 59, no. 2, pp. 928-941, 2012.

[7] Bhowal K., Sarkar D., Biswas S., and Sarkar P., "An Efficient Steganographic Approach to Hide Information in Digital Audio Using Modulus Operation," *The International Arab Journal of Information Technology*, vol. 16, no. 4, pp. 703-711, 2019.

[8] Clancy S. and Brown W., "Translation: DNA to mRNA to Protein," *Nature Education*, vol. 1, no. 1, pp. 101, 2008.

[9] Deepikaa S. and Saravanan R., "VoIP Steganography Methods, a Survey," *Cybernetics and Information Technologies*, vol. 19, no. 1, pp. 73-87, 2019.

[10] Deepikaa S. and Saravanan R., "Coverless VoIP Steganography Using Hash and Hash," *Cybernetics and Information Technologies*, vol. 20, no. 3, pp. 102-115, 2020.

[11] Djebbar F., Ayad B., Meraim K., and Hamam H., "Comparative Study of Digital Audio Steganography Techniques," *EURASIP Journal on Audio, Speech, and Music Processing*, vol. 2012, no. 1, pp 1-16, 2012.

[12] Farhan A., Ali R., Yassein H., Al-Saidi N., and Abdul-Majeed G., "A New Approach to Generate Multi S-Boxes Based on RNA Computing," *International journal of innovative computing, information and control: IJICIC*, vol. 16, no. 1, pp. 331-348, 2020.

[13] Hamed G., Marey M., El-Sayed S., and Tolba F., *Applications of Intelligent Optimization in Biology and Medicine*, Springer, 2016.

[14] Jayaram P., Ranganatha H., and Anupama H., "Information Hiding Using Audio Steganography-A Survey," *The International Journal of Multimedia and its Applications*, vol. 3, no. 3, pp. 86-96, 2011.

[15] Jenifer J., Ratna S., Loret J., and Gethsy D., "A Survey on Different Video Steganography Techniques," *in Proceedings of 2nd International Conference on Trends in Electronics and* Informatics, Tirunelveli, pp. 627-632, 2018.

[16] Kadhim I., Premaratne P., Vial P., and Halloran B., "Comprehensive Survey of Image Steganography: Techniques, Evaluations, and Trends in Future Research," *Neurocomputing*, vol. 335, pp. 299-326, 2019.

[17] Lubacz J., Mazurczyk W., and Szczypiorski K., "Principles and Overview of Network Steganography," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 225-229, 2014.

[18] Malathi P., Manoaj M., Manoj R., Raghavan V., and Vinodhini R., "Highly Improved DNA Based Steganography," *Procedia Computer Science*, vol. 115, pp. 651-659, 2017.

[19] Marwan S., Shawish A., and Nagaty K., "An Enhanced DNA-based Steganography Technique with a Higher Hiding Capacity," *Bioinformatics*, pp. 150-157, 2015.

[20] Mazurczyk W. and Lubacz J., "LACK—A Voip Steganographic Method," *Telecommunication Systems*, vol. 45, no. 2-3, pp. 153-163, 2010.

[21] Mazurczyk W., Smolarczyk M., and Szczypiorski K., "Retransmission Steganography and its Detection.," *Soft Computing*, vol. 15, no. 3, pp. 505-515, 2011.

[22] Mazurczyk W., "Voip Steganography and Its Detection-A Survey," *ACM Computing Surveys*, vol. 46, no. 2, pp. 1-21, 2013.

[23] Mitras B. and Aboo A., "Proposed Steganography Approach Using DNA Properties," *International Journal of Information Technology and Business Management*, vol. 14, no. 1, pp. 96-102, 2013.

[24] Mohammed M., Taloba A., and Ali B., "DNA-Based Steganography Using Neural Networks," *in Proceedings of International Japan-Africa Conference on Electronics, Communications and Computations*, Alexandria, pp. 79-82, 2018.

[25] Na D., "DNA Steganography: Hiding Undetectable Secret Messages within the Single Nucleotide Polymorphisms of A Genome and Detecting Mutation-Induced Errors," *Microbial Cell Factories*, vol. 19, no. 1, pp. 1-9, 2020.

[26] Nisperos Z., Gerardo B., and Hernandez A., "A Coverless Approach to Data Hiding Using DNA Sequences," *in Proceedings of 2nd World Symposium on Communication Engineering*, Nagoya, pp. 21-25, 2019.

[27] Qin J, Tian H., Huang Y., Liu J., Chen Y., Wang T., Cai Y., and Wang X., "An Efficient Voip Steganography based on Random Binary Matrix," *in Proceedings of 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, Krakow, pp. 462-465, 2015.

[28] Salomon D., *Data Compression: The Complete Reference*, Springer, 2012.

[29] Shiu H., Ng K., Fang J., Lee R., and Huang C., "Data Hiding Methods Based Upon DNA Sequences," *Information Sciences*, vol. 180, no. 11, pp. 2196-2208, 2011.

[30] Sushma R., Namitha M., Manjula G., Johar S., and Hiriyanna G., "DNA based Steganography Using 2-3-3 Technique," *in Proceedings of International Conference on Data Science and Communication*, Bangalore, pp. 1-6, 2019.

[31] Tian H., Jiang H., Zhou K., and Feng D., "Adaptive Partial-Matching Steganography For Voice Over IP Using Triple M Sequences," *Computer Communications*, vol. 34, no. 18, pp. 2236-2247, 2011.

[32] Tian H., Qin J., Guo S., Huang Y., Liu J., Wang T., ChenY., and Cai Y., "Improved Adaptive Partial-Matching Steganography for Voice Over IP," *Computer Communications*, vol. 70, pp. 95-108, 2015.

[33] Tian H., Liu J., and Li S., "Improving Security of Quantization-Index-Modulation Steganography in Low Bit-Rate Speech Streams," *Multimedia Systems*, vol. 20, no. 2, pp. 143-154, 2014.

[34] Tian H., Qin J., Huang Y., Chen Y., Wang T., Liu J., and Cai Y., "Optimal Matrix Embedding for Voice-Over-IP Steganography," *Signal Processing*, vol. 117, pp. 33-43, 2017.

[35] Wang Z., Zhao X., Wang H., and Cui G., "Information Hiding Based on DNA Steganography," *in Proceedings of IEEE 4th International Conference on Software Engineering and Service Science*, Beijing, pp. 946-949, 2013.

[36] Wu K. and Wang C., "Steganography Using Reversible Texture Synthesis," *IEEE Transactions on Image Processing*, vol. 24, no. 1, pp. 130-139, 2015.

[37] Xu J., Mao X., Jin X., Jaffer A., Lu S., Li L., and Toyoura M., "Hidden Message In A Deformation-Based Texture," *The Visual Computer*, vol. 31, no. 12, pp. 1653-1669, 2015.

[38] Zhang X., Peng F., and Long M., "Robust Coverless Image Steganography Based on DCT and LDA Topic Classification," *IEEE Transactions on Multimedia*, vol. 20, no. 12, pp. 3223-3238, 2018.

[39] Zheng S., Wang L., Ling B., and Hu D., "Coverless Information Hiding Based on Robust Image Hashing," *in Proceedings of International Conference on Intelligent Computing*, pp. 536-547, 2017.

[40] Zhou Z., Sun H., Harit R., Chen X., and Sun X., "Coverless Image Steganography without Embedding," *in Proceedings of International Conference on Cloud Computing and Security*, Nanjing, pp. 123-132, 2015.

[41] Zhou Z., Mu Y., and Wu Q., "Coverless Image Steganography Using Partial-Duplicate Image Retrieval," *Soft Computing*, vol. 23, no. 13, pp. 4927-4938, 2019.

[42] Zou L., Sun J., Gao M., Wan W., and Gupta B., "A Novel Coverless Information Hiding Method Based on the Average Pixel Value of the Sub-Images," *Multimedia Tools and Applications*, vol. 78, no. 7, pp. 7965-7980, 2019.

Deepikaa Soundararajan received her MS in Software Engineering from Vellore Institute of Technology, Vellore, India. She is pusuing her Ph.d work in Vellore Institute of Technology, Vellore Her research interest includes Networks, wireless network security, especially Steganography.

Saravanan Ramakrishnan completed his Ph.D. degree from University of Madras. He has about two decades of teaching and rich research experience. His areas of research include mobile computing, approximation algorithms, cryptography and network security.